North Carolina Security Breach Reporting Form
Pursuant to the Identity Theft Protection Act of 2005

*Indicated a mandatory field

*Name of the Company or Government Agency owning or licensing information affected by the entity experiencing breach:

POSTERNAK BLANKSTEIN & LUND, LLP

Entity Type:	GENERAL BUSINESS
Address:	
Apt/Suite/Building:	
City:	
State:	
Zip Code:	
Telephone:	
Fax:	
Email:	

*Date Security breach Reporting Form Submitted:	08/31/2018
Is this notice a supplement to a previously filed Security Breach:	NO
*Date the Security Breach was discovered:	06/29/2018
Breach Type:	PHISHING
*Estimated number of affected individuals:	177
*Estimated number of NC residents affected:	1

Name of company or government agency maintaining or possessing information that was the subject of the Security Breach, if the agency that experienced the Security Breach is not the same entity as the agency reporting the Security Breach (pursuant to N.C.G.S. 75-65(b))

N/A

Describe the circumstances surrounding the Security Breach:

ON JUNE 29, 2018, POSTERNAK BLANKSTEIN & LUND, LLP ("POSTERNAK"), LEARNED THROUGH A FORENSIC INVESTIGATION INTO A PHISHING INCIDENT THAT AN UNKNOWN INDIVIDUAL HAD GAINED ACCESS TO A POSTERNAK EMPLOYEE'S EMAIL ACCOUNT. ON JULY 30, 2018, POSTERNAK LEARNED THE IDENTITIES OF THE INDIVIDUALS WHOSE PERSONAL INFORMATION WAS IN THE EMPLOYEE'S EMAIL ACCOUNT AND WHAT INFORMATION MAY HAVE BEEN AFFECTED. ALTHOUGH, TO DATE, POSTERNAK DOES NOT KNOW IF ANY SENSITIVE PERSONAL INFORMATION WAS ACCESSED WITHOUT PERMISSION, IT IS PROVIDING NOTIFICATION TO POTENTIALLY AFFECTED INDIVIDUALS OUT OF AN ABUNDANCE OF CAUTION. THE INFORMATION THAT COULD HAVE BEEN ACCESSED IN THE EMPLOYEE'S ACCOUNT INCLUDES THE NAME AND FINANCIAL ACCOUNT AND ROUTING NUMBER FOR ONE NORTH CAROLINA RESIDENT. ON AUGUST 31, 2018, POSTERNAK WILL BEGIN MAILING WRITTEN NOTIFICATIONS TO POTENTIALLY AFFECTED INDIVIDUALS. POSTERNAK HAS ALSO PROVIDED A TELEPHONE NUMBER FOR POTENTIALLY AFFECTED INDIVIDUALS TO CALL WITH ANY QUESTIONS THEY MAY HAVE.

Information Type:	ACCOUNT #
*Regarding information breached, if electronic, was the information protected in some manner:	YES
If YES, please describe the security measures protecting the information:	THE INFORMATION WAS PROTECTED THROUGH PASSWORDS ON A PROFESSIONALLY HOSTED EMAIL PLATFORM.
*Describe any measures taken to prevent a similar Security Breach from occurring in the future:	TO HELP PREVENT SOMETHING LIKE THIS FROM HAPPENING IN THE FUTURE, POSTERNAK HAS TAKEN STEPS TO ENHANCE ITS EXISTING NETWORK AND EMAIL SECURITY, INCLUDING PROVIDING CONTINUED TRAINING TO THEIR EMPLOYEES ON DATA SECURITY AND THE DANGERS OF PHISHING EMAILS AND IMPLEMENTING MULTI-FACTOR AUTHENTICATION.
*Date affected NC residents were/will be notified:	08/31/2018
Describe the circumstances surrounding the delay in notifying affected NC residents pursuant to N.C.G.S. 75-65 (a) and (c):	NOTICE IS BEING PROVIDED IN THE MOST EXPEDITIOUS TIME POSSIBLE AND WITHOUT UNREASONABLE DELAY.

If the delay was pursuant to a request from law enforcement pursuant to N.C.G.S. 75-65(c), please attach or mail the written request or the contemporaneous memorandum.

How NC residents were/will be notified? (pursuant to N.C.G.S. 75-65 (e)):	WRITTEN NOTICE

Please note if the business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000) or that the affected class of subject persons to be notified exceeds 500,000, or if the business does not have sufficient contact information or consent to satisfy subdivisions (1), (2) , or (3) of this subsection, for only those affected persons without sufficient contact

information or consent, or if the business is unable to identify particular affected persons, for only those unidentifiable affected persons. Substitute notice shall consist of all the following:

- Email notice when the business has an electronic mail address for the subject persons
- Conspicuous posting of the notice on the Web site page of the business, if one is maintained
- Notification to major statewide media

Please attach a copy of the notice if in written form or a copy of any scripted notice if in telephonic form.

Contact Information Affiliation with entity experiencing breach:	ATTORNEY		
Organization Name:	BAKER & HOSTETLER LLP		
Prefix:	MR		
*First Name:	DAVID		
Middle Name:			
*Last Name:	KITCHEN		
Suffix:			
Title:	PARTNER		
Address:	127 PUBLIC SQUARE		
Apt/Suite/building:	SUITE 2000		
City:	CLEVELAND		
State:	OH	Zip Code:	44114
*Telephone:	(216) 621-0200	Fax:	
Email:	DKITCHEN@BAKERLAW.COM		

Appendix

On June 29, 2018, Posternak Blankstein & Lund, LLP ("Posternak"), learned through a forensic investigation into a phishing incident, that an unknown individual had gained access to a Posternak employee's email account. On July 30, 2018, Posternak learned the identities of the individuals whose personal information was in the employee's email account and what information may have been affected. Although, to date, Posternak does not know if any sensitive personal information was accessed without permission, it is providing notification to potentially affected individuals out of an abundance of caution. The information that could have been accessed in the employee's account include the name and financial account and routing numbers for one (1) North Carolina resident.

On August 31, 2018, Posternak will begin mailing written notifications to potentially affected individuals. These individuals include one North Carolina resident who is being notified of the incident in writing in accordance with N.C. Gen. Stat. §§ 75-65 in substantially the same form as the enclosed letter.[1] Posternak has also provided a telephone number for potentially affected individuals to call with any questions they may have.

To help prevent something like this from happening in the future, Posternak has taken steps to enhance its existing network and email security, including providing continued training to their employees on data security and the dangers of phishing emails.

[1] This report does not waive Posternak's objection that North Carolina lacks personal jurisdiction regarding the company related to this matter.

Posternak
POSTERNAK BLANKSTEIN & LUND LLP

Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

[redacted]

August 31, 2018

Dear [redacted]:

Posternak Blankstein & Lund LLP ("Posternak") understands the importance of protecting individuals' personal information. We are writing to inform you that we recently identified and addressed a security incident that may have involved your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

On June 29, 2018, we learned through an ongoing forensic investigation into a phishing incident that an unauthorized party had obtained access to an email account belonging to a Posternak attorney. Upon first learning of the phishing incident, we immediately secured and enhanced security for the employee account, changed the account password, and commenced an internal investigation. We also engaged a professional forensic security firm to assist with the investigation. The investigation determined that an unauthorized person had accessed the employee email account, but the investigation was unable to determine the scope of information that may have been accessed or acquired. While we have no indication that your information has been misused, we are providing you this notice out of an abundance of caution so that you understand the nature of your information that was contained in the email account and can take steps to help protect yourself. The email account contained documents transmitted by debtors or lawyers involved in bankruptcy matters and which contained your name and a financial account number and routing number for a [redacted] account.

We encourage you to remain vigilant by reviewing your account statements and free credit reports for any unauthorized activity. We recommend that you monitor your account statements for any unauthorized activity and report any suspected fraud to your banking institution and card issuer immediately. Card network rules generally provide that cardholders are not responsible for unauthorized charges that are reported promptly. The phone number to call is usually on the back of your payment card. Please see the pages that follow for additional steps you can take to protect your information.

We apologize for any inconvenience caused by this incident. To help prevent this type of incident from happening again, we are taking significant steps to enhance our existing data security procedures and providing continued training to our employees on data security and the dangers of phishing emails. If you have questions, please call at 877-588-5667, Monday through Friday between 9:00 am and 9:00 pm Eastern Time.

Sincerely,

Adam J. Ruttenberg, Partner
Posternak Blankstein & Lund LLP

MORE INFORMATION ON WAYS TO PROTECT YOURSELF

We recommend that you remain vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
Experian, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

Federal Trade Commission, Consumer Response Center**,** 600 Pennsylvania Avenue, NW Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.gov/idtheft

If you are a resident of Connecticut, Maryland, or North Carolina you may contact and obtain information from your state attorney general at:

Connecticut Attorney General's Office, 55 Elm Street, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag

Maryland Attorney General's Office, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023 (toll free when calling within Maryland)
(410) 576-6300 (for calls originating outside Maryland)

North Carolina Attorney General's Office, 9001 Mail Service Center, Raleigh, NC 27699, www.ncdoj.gov, 1-877-566-7226

Fraud Alerts: There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least 90 days. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Credit Freezes: You may have the right to put a credit freeze, also known as a security freeze, on your credit file, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A credit freeze is designed to prevent potential credit grantors from accessing your credit report without your consent. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a credit freeze may delay your ability to obtain credit. In addition, you may incur fees to place, lift and/or remove a credit freeze. Credit freeze laws vary from state to state. The cost of placing, temporarily lifting, and removing a credit freeze also varies by state, generally $5 to $20 per action at each credit reporting company. Unlike a fraud alert, you must separately place a credit freeze on your credit file at each credit reporting company. Since the instructions for how to establish a credit freeze differ from state to state, please contact the three major credit reporting companies as specified below to find out more information.

To place a security freeze on your credit report, you must send a written request to each of the three major reporting agencies by regular, certified, or overnight mail at the addresses below:

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com
Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com
TransUnion Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
1. Social Security number
2. Date of birth
3. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years
4. Proof of current address such as a current utility bill or telephone bill
5. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
6. If you are a victim of identity theft, include a copy of the police report, investigative report, or complaint to a law enforcement agency concerning identity theft

The credit reporting agencies have three (3) business days after receiving your request to place a security freeze on your credit report. The credit bureaus must also send written confirmation to you within five (5) business days and provide you with a unique personal identification number ("PIN") or password or both that can be used by you to authorize the removal or lifting of the security freeze.

To lift the security freeze in order to allow a specific entity or individual access to your credit report, you must call or send a written request to the credit reporting agencies by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze as well as the identity of those entities or individuals you would like to receive your credit report or the specific period of time you want the credit report available. The credit reporting agencies have three (3) business days after receiving your request to lift the security freeze for those identified entities or for the specified period of time.

To remove the security freeze, you must send a written request to each of the three credit bureaus by mail and include proper identification (name, address, and Social Security number) and the PIN number or password provided to you when you placed the security freeze. The credit bureaus have three (3) business days after receiving your request to remove the security freeze.